



ATA DA 82ª (OCTAGÉSIMA SEGUNDA) REUNIÃO ORDINÁRIA DO
COMITÊ DE AUDITORIA ESTATUTÁRIO – CAE

1 – Data, hora e local da realização:

Reunião realizada no dia 24 (vinte quatro) do mês de novembro de 2021. Em atendimento às recomendações contidas nos Decretos nº 64.862/2020 e 64.864/2020, que tratam de medidas temporárias e emergenciais de prevenção de contágio pelo COVID-19, a 82ª Reunião Ordinária do Comitê de Auditoria Estatutário – CAE, de modo “virtual”, por vídeo conferência, Microsoft Teams – 9h00 às 12h horas.

2 – Participantes:

Afonso Antonio Hennel – membro do CAE
Elionor Farah Jreige Weffort – Coordenadora do CAE
Silverio Crestana – membro do CAE

Secretaria de Governança:

- Carolina Vilela Santoro de Castro Vianna Jacob
- Leila Cristina P. R. Serrano
- Lara de Moraes Forjaz- convidada

3 - Assuntos:

3.1 – Planejamento e aprovação das Atas do CAE

Os membros do CAE se reuniram sem a presença da secretaria para a discussão e tratativas sobre as matérias que serão objeto de análise nas reuniões do dia de trabalho.

3.2 - Gerência de Conformidade, Controles Internos e Riscos

– Sérgio de Carvalho Junior

Análise do Relatório Mensal da GRI – Destaques:

- Manual de Políticas e Práticas da empresa;
- Monitoramento dos riscos identificados e as ações para mitigar os efeitos;
- Relatório de Atividades da GRI – Anual

Documentos disponibilizados:

- Relatório Trimestral GRI;
- Riscos Empresariais.

Tendo em vista a disponibilização do material com antecedência, o CAE solicitou que a exposição seja somente sobre os pontos de destaque para a discussão.

Relatório Trimestral

O Sr. Sérgio de Carvalho Junior – GRI iniciou a apresentação informando que o modelo de relatório apresentado é igual ao encaminhado ao CODEC para atendimento à Deliberação CODEC nº 02/2018, portanto questiona se existe a necessidade de alteração no modelo apresentado ao CAE.

Com relação a Matriz de Risco foi destacado que:

- A empresa está mobilizada na finalização da Matriz de Risco. O avanço é visível, tendo em vista que toda a construção da matriz de risco apresentada foi realizada

de "forma caseira" e sem recursos adicionais. A apresentação e discussão sobre o tema demonstraram que a Companhia tem como identificar as fontes de risco e os responsáveis por cada um dos riscos empresariais apontados.

- Em relação ao cronograma de ações da matriz de risco, a previsão é de que ocorra, no 1º semestre de 2022, a definição dos indicadores de riscos empresariais e o lançamento do Sistema de Gestão de Riscos – SGR, ferramenta desenvolvida internamente. Foram identificados 12 grandes riscos empresariais, o mapa de calor foi concluído e encontra-se em fase de produção dos indicadores e identificação das ações mitigadoras.
- A matriz de Risco já conta com a identificação da área gestora e os responsáveis pelas tarefas que influenciam no seu resultado direto.
- A contratação da consultoria para auxiliar a CPTM no desenvolvimento da Matriz de Riscos ainda não foi efetivada em virtude da demora na liberação pelo COETIC e espera que o edital seja publicado em breve. Adicionalmente informou que a valoração da contratação da consultoria, elaborada pela Gerência de Custos foi muito boa e contou com a ajuda da Gerência de Tecnologia da Informação – GFI na construção das especificações técnicas necessárias.

Com relação as políticas os destaques foram: a criação da Gerência de Governança e o Comitê de Governança; o acompanhamento das políticas aprovadas e das que estão em revisão e; a revisão do CCI que tem pautado toda a gestão da Companhia; a revisão de todo o sistema normativo que detalham e operacionalizam as políticas da Companhia.

Comentários e Sugestões do CAE

O CAE agradeceu a apresentação do Sr. Sérgio. Em relação ao relatório da GRI, o CAE entendeu que é necessária a manutenção do relatório mensal, de modo a possibilitar, neste momento, o acompanhamento mês a mês da construção da matriz de risco da Companhia. Sobre a matriz de riscos, o CAE: i. reconheceu e parabenizou os esforços da equipe da GRI no desenvolvimento da matriz e na busca por soluções alternativas para superar as dificuldades, tendo em vista que todo o trabalho foi realizado de forma caseira e com recursos próprios, que são limitados; ii. observou que os resultados obtidos até o momento geram estímulos aos colaboradores; iii. reforçou a necessidade de buscar suporte em uma consultoria externa que permita um salto de qualidade e aprimoramento do que foi desenvolvido internamente, em especial para orientar na análise e detalhamento dos riscos; iv. sugeriu que a GRI faça contatos com outras empresas do Estado que já contrataram este tipo de consultoria para assegurar que o Edital e a empresa contratada efetivamente atendam às necessidades da Companhia; v. recomendou a compra de um sistema de gestão de riscos com ferramentas mais robustas que facilite a integração com as áreas e; vi. recomendou que a CPTM procure o órgão controlador – CODEC quando da discussão do apetite ao risco, tendo em vista a participação societária do Estado na Companhia.

Em relação às políticas e normativos que orientam sua implementação, o CAE sugeriu a contratação de uma consultoria para mapeamento de conformidade das políticas e na orientação de sua implantação.

3.3 – Auditoria

- Juliana Stark – DRAU

- **Supervisão da Auditoria Interna:**

- Relato dos Trabalhos de Auditoria Interna em andamento no mês;

Documentos disponibilizados:

- DRAU - Atividades até 16-11-2021

Tendo em vista a disponibilização do material com antecedência, o CAE solicitou que a exposição seja somente sobre os pontos de destaque para a discussão. A Sra. Juliana Stark – DRAU iniciou a apresentação destacando os principais aspectos do PAINT 2022:

- Já abrange a matriz de riscos, tendo em vista a finalização pela GRI;
- O PAINT está no 3º ano do ciclo;
- A Revisão dos objetos auditáveis que passaram de 119 para 89;
- Os critérios foram mantidos;
- Definição dos riscos sob a ótica da auditoria: relevância, criticidade e maturidade;
- Utilização de uma classificação conservadora dos processos selecionados para auditoria, que foi semelhante à percepção da Diretoria;
- 49 objetos selecionados para auditoria em 2022;
- O Contrato do CBTC está destacado para realização de auditoria conforme orientação do CAE;
- Prevista Auditoria nos controles, aquisição e fornecimento de EPI envolvendo o almoxarifado e o recursos humanos;
- Controle sobre o registro de frequência e horas extras, que abrange o trabalho remoto;
- Auditorias contínuas em andamento e;
- Controle no uso de drones e fiscalização de portarias.

Comentários e Sugestões do CAE

O CAE destacou a posição do CODEC, conforme explanado na reunião de Comitês de Auditoria realizada no âmbito de todo o Estado, sobre a necessidade de uma gestão patrimonial mais efetiva. Informado da existência de um Grupo de Trabalho Interno, o CAE solicita que seja agendada uma apresentação para tratar do assunto, incluindo a questão das concessões. Reconheceu que o Plano Anual de Auditoria está bem abrangente, mas destaca sua preocupação com as transações entre partes relacionadas e orienta que tão logo as diretrizes/regramento sejam estabelecidas em norma específica, a Auditoria deverá incluir no respectivo plano anual.

Manteve, ainda, a recomendação permanente da necessidade de emprego de automação e inteligência artificial nos trabalhos de auditoria, tendo em vista a grande quantidade de transações e contratos a serem auditados, bem como a capacitação constante da equipe com vistas, entre outros aspectos, à busca de certificação da Auditoria Interna da CPTM junto ao IIA.

3.4 – Canal de Denúncias / Ouvidoria / Comitê de Ética

- Sergio de Carvalho Junior – Coordenador do Comitê de Ética

- Supervisionar o Canal de Denúncias, Ouvidoria, Comitê de Ética: Ocorrências e soluções.

Documentos disponibilizados:

- Relatório Comitê de Ética OUTUBRO.

A Dra. Carolina – GRG mostrou as providências e as ferramentas que estão sendo adotadas para o acesso dos membros do CAE ao Canal de Denúncias, bem como a criação de um e-mail “Fale com o CAE”, o que permitirá que o Comitê receba denúncias. Foi informado que o acesso ao Canal de Denúncias deverá se dar em ambiente da Companhia.

O Sr. Sérgio de Carvalho Junior – GRI ingressou à reunião e iniciou a exposição, destacando os seguintes pontos: i) Fluxo das demandas e, ii) Acesso ao canal, conforme exposto pela Dra. Carolina.

Comentários e Sugestões do CAE

Em síntese, o CAE: i. reforçou a relevância do canal de denúncias e a necessidade de assegurar o seu funcionamento adequado; ii. manifestou dúvidas com relação ao fluxo das demandas que poderão entrar pela via do e-mail “Fale com o CAE”, o que não é muito claro em se tratando de empresa estatal e, neste sentido, entende que o apoio da Gerência Jurídica, do CODEC e do Grupo de Governança existente no âmbito do Conselho de Administração são importantes para delimitar o que atribuição do CAE; iii. ressaltou a necessidade, no Canal de Denúncias, de um fluxo pré-estabelecido para as denúncias consideradas relevantes de forma que elas cheguem ao CAE e CA para o efetivo acompanhamento, contemplando, entre outros aspectos, filtros que considerem o tipo de conduta, gravidade e posição do denunciado, instituindo procedimentos que tragam segurança para todos.

3.5 – Cyber Security

- André de Almeida Catarino Pereira – Gerente de Tecnologia da Informação.
- Carlos Alberto Tubertini – Assessor da Gerência de Tecnologia da Informação

Medidas relativas à Cyber Security

Documentos disponibilizados:

- CIA_v05 - Segurança da Informação.

Tendo em vista que o material foi disponibilizado com antecedência, a apresentação foi dispensada e o Senhor Carlos Alberto Tubertini destacou somente os principais pontos, conforme abaixo:

- A Política de Segurança da Informação já foi elaborada e está aguardando a validação para a devida publicação;
- Apresentou os dados do ambiente tecnológico: i) dados da equipe; ii) servidores e redes; iii) serviços.
- Confidencialidade com senhas seguras para acesso aos dados e sistemas;
- Controle de acesso normatizado e com assinatura de termo de responsabilidade diário;
- Controle de acesso externo realizado pela VPN ou site seguro;
- Para todos os parceiros externos têm cláusula de confidencialidade prevista no CCI;
- Acessos aos sistemas são definidos e aprovados pelo gestor da área responsável;
- Auditoria realizada anualmente pela empresa contratada;
- Não houve “pichações” ou sucesso de ataques – sites seguros;
- Há realização constante de testes de invasão;
- Disponibilidade de: i) sala cofre certificada; ii) alta disponibilidade – redundância; iii) disponibilidade de internet, intranet e de sistemas críticos acima de 99%;
- Aparato de segurança, na visão dele, muito robusto com: i) Firewall Proxy; ii) Antivírus; iii) AntiSpam;
- O mapa da riscos da TI já foi elaborado e estão sendo trabalhadas as ações mitigadoras para cada risco identificado;
- Cyber Segurança na Pandemia: i) home office implantado em março/2020; ii) VPN suportou e vem suportando de acordo; iii) utilização da ferramenta “Teams” e; iv) acompanhamento constante.

Sobre a LGPD, informou as seguintes ações: i) mapeamento de todos os riscos e identificação das ações mitigadoras para os riscos mapeados; ii) Implantação do canal de comunicação da LGPD; iii) identificação de todos os processos; iv) coleta dos dados; v) revisão/adequação das normas vigentes; vi) identificação de soluções para segurança de LGPD e; vii) realização do curso sobre LGPD.

O Sr. André – GFI fez as considerações finais destacando as necessidades e principais realizações da Gerência de Tecnologia da Informação: i) existe a previsão de grande investimento no parque tecnológico da Companhia; ii) implantação do datacenter redundante; iii) atualização tecnológica; iv) previsão orçamentária para a tecnologia da informação em 2022 na ordem de R\$ 7,5 milhões e; v) aquisição de novo ERP previsto para o 1º trimestre de 2022.

Comentários e Sugestões do CAE

O CAE agradeceu a apresentação e reforçou a necessidade da aquisição do novo ERP para a área financeira e contábil, melhorando a performance das áreas envolvidas, principalmente com a eliminação de lançamentos manuais que geram riscos à Companhia. Destacou, ainda, a necessidade de manutenção dos testes e outras medidas para evitar cyber ataques, incluindo a previsão explícita de um plano de crise em caso de ocorrência.

4 - Pendências:

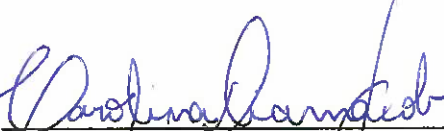
PENDÊNCIAS	
Assuntos	Responsável
Pautar para próxima reunião o assunto sobre Gestão Patrimonial	Secretaria de Governança

NADA MAIS havendo a tratar, foi encerrada a reunião e lavrada a presente ata.


ELIONOR FARAH JREIGE WEFFORT
Coordenadora


AFONSO ANTONIO HENNEL
Membro


SILVERIO CRESTANA
Membro


CAROLINA VILELA SANTORO DE
CASTRO VIANNA JACOB
Secretária